

CLAIMS

What is claimed is:

- 1 1. A method of reporting malware events comprising the steps of:
 - 2 detecting a malware event;
 - 3 determining a level of the detected malware event;
 - 4 comparing the level of the detected malware event to an event trigger
 - 5 threshold; and
 - 6 transmitting a notification of the detected malware event, based on the
 - 7 comparison of the level of the detected malware event to the event trigger
 - 8 threshold.
- 1 2. The method of claim 1, wherein the detecting step comprises the step of:
 - 2 detecting the malware event using a malware scanner.
- 1 3. The method of claim 2, wherein the malware event comprises at least one
 - 2 of:
 - 3 completion of a malware scan, a process failure relating to malware
 - 4 scanning, a missing log file, detection of a malware, or failure of a response to a
 - 5 malware.

1 4. The method of claim 1, wherein the malware event has one of a plurality
2 of levels.

1 5. The method of claim 4, wherein the level of the malware event comprises
2 one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 6. The method of claim 5, wherein the event trigger threshold comprises one
2 of a plurality of levels.

1 7. The method of claim 6, wherein the level of the event trigger threshold
2 comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events

6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 8. The method of claim 7, wherein the malware event comprises at least one
2 of:

3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 9. The method of claim 1, wherein the transmitting step comprises the steps
2 of:

3 transmitting the notification of the detected malware event in real-time, if
4 the level of the detected malware event is greater than or equal to the event
5 trigger threshold; and

6 transmitting the notification of the detected malware event eventually, if
7 the level of the detected malware event is less than the event trigger threshold.

1 10. The method of claim 9, wherein the malware event has one of a plurality
2 of levels.

1 11. The method of claim 10, wherein the level of the malware event
2 comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 12. The method of claim 11, wherein the event trigger threshold comprises
2 one of a plurality of levels.

1 13. The method of claim 12, wherein the level of the event trigger threshold
2 comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 14. The method of claim 13, wherein the malware event comprises at least
2 one of:

3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 15. The method of claim 14, wherein the detecting step comprises the step of:
2 detecting the malware event using a malware scanner.

1 16. The method of claim 15, wherein the method further comprises the step
2 of:
3 transmitting an alert to an administrator indicating occurrence of the
4 detected malware event in real-time, if the level of the detected malware event is
5 greater than or equal to the event trigger threshold.

1 17. A system for reporting malware events comprising:
2 a processor operable to execute computer program instructions;
3 a memory operable to store computer program instructions executable
4 by the processor; and

5 computer program instructions stored in the memory and executable to
6 perform the steps of:
7 detecting a malware event;
8 determining a level of the detected malware event;
9 comparing the level of the detected malware event to an event trigger
10 threshold; and
11 transmitting a notification of the detected malware event, based on the
12 comparison of the level of the detected malware event to the event trigger
13 threshold.

1 18. The system of claim 17, wherein the detecting step comprises the step of:
2 detecting the malware event using a malware scanner.

1 19. The system of claim 18, wherein the malware event comprises at least one
2 of:
3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 20. The system of claim 17, wherein the malware event has one of a plurality
2 of levels.

1 21. The system of claim 20, wherein the level of the malware event comprises
2 one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 22. The system of claim 21, wherein the event trigger threshold comprises one
2 of a plurality of levels.

1 23. The system of claim 22, wherein the level of the event trigger threshold
2 comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events

6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 24. The system of claim 23, wherein the malware event comprises at least one
2 of:

3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 25. The system of claim 17, wherein the transmitting step comprises the steps
2 of:

3 transmitting the notification of the detected malware event in real-time, if
4 the level of the detected malware event is greater than or equal to the event
5 trigger threshold; and

6 transmitting the notification of the detected malware event eventually, if
7 the level of the detected malware event is less than the event trigger threshold.

1 26. The system of claim 25, wherein the malware event has one of a plurality
2 of levels.

1 27. The system of claim 26, wherein the level of the malware event comprises
2 one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 28. The system of claim 27, wherein the event trigger threshold comprises one
2 of a plurality of levels.

1 29. The system of claim 28, wherein the level of the event trigger threshold
2 comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 30. The system of claim 29, wherein the malware event comprises at least one
2 of:

3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 31. The system of claim 30, wherein the detecting step comprises the step of:
2 detecting the malware event using a malware scanner.

1 32. The system of claim 31, further comprising the step of:
2 transmitting an alert to an administrator indicating occurrence of the
3 detected malware event in real-time, if the level of the detected malware event is
4 greater than or equal to the event trigger threshold.

1 33. A computer program product for reporting malware events, comprising:
2 a computer readable medium;
3 computer program instructions, recorded on the computer readable
4 medium, executable by a processor, for performing the steps of
5 detecting a malware event;
6 determining a level of the detected malware event;

7 comparing the level of the detected malware event to an event trigger
8 threshold; and
9 transmitting a notification of the detected malware event, based on the
10 comparison of the level of the detected malware event to the event trigger
11 threshold.

1 34. The computer program product of claim 33, wherein the detecting step
2 comprises the step of:
3 detecting the malware event using a malware scanner.

1 35. The computer program product of claim 34, wherein the malware event
2 comprises at least one of:
3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 36. The computer program product of claim 33, wherein the malware event
2 has one of a plurality of levels.

1 37. The computer program product of claim 36, wherein the level of the
2 malware event comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 38. The computer program product of claim 37, wherein the event trigger
2 threshold comprises one of a plurality of levels.

1 39. The computer program product of claim 38, wherein the level of the event
2 trigger threshold comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 40. The computer program product of claim 39, wherein the malware event
2 comprises at least one of:
3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 41. The computer program product of claim 33, wherein the transmitting step
2 comprises the steps of:
3 transmitting the notification of the detected malware event in real-time, if
4 the level of the detected malware event is greater than or equal to the event
5 trigger threshold; and
6 transmitting the notification of the detected malware event eventually, if
7 the level of the detected malware event is less than the event trigger threshold.

1 42. The computer program product of claim 41, wherein the malware event
2 has one of a plurality of levels.

1 43. The computer program product of claim 42, wherein the level of the
2 malware event comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 44. The computer program product of claim 43, wherein the event trigger
2 threshold comprises one of a plurality of levels.

1 45. The computer program product of claim 44, wherein the level of the event
2 trigger threshold comprises one of:

3 informational malware events requiring no operator intervention; warning
4 malware events that indicate a process failure; minor malware events that require
5 attention, but are not events that could lead to loss of data; major malware events
6 that need operator attention; critical malware events that need immediate operator
7 attention and could lead to loss of data if not corrected.

1 46. The computer program product of claim 45, wherein the malware event
2 comprises at least one of:

3 completion of a malware scan, a process failure relating to malware
4 scanning, a missing log file, detection of a malware, or failure of a response to a
5 malware.

1 47. The computer program product of claim 46, wherein the detecting step
2 comprises the step of:

3 detecting the malware event using a malware scanner.

1 48. The computer program product of claim 47, further comprising the step
2 of:

3 transmitting an alert to an administrator indicating occurrence of the
4 detected malware event in real-time, if the level of the detected malware event is
5 greater than or equal to the event trigger threshold.